UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

FILED
08 MAR 21 PM 4:33
CLERK, U.S. DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA
BY DEPUTY

In the Matter of the Search of
(Name, address or brief description of person, property or premises to be searched)

"Notebook" Laptop Computer
Model M54G "Alienware"
Serial number KA61N4N1N298

APPLICATION AND AFFIDAVIT
FOR SEARCH WARRANT

Case Number: ~~08MJ0622~~ '08 MJ 0895

I, Kevin J. Straus being duly sworn depose and say:

I am a(n) Special Agent of the Federal Bureau of Investigation and have reason to believe
Official Title

that ☐ on the person of or ☑ on the property or premises known as (name, description and/or location)

See Attachment A (incorporated by reference herein)

in the Southern District of California

there is now concealed a certain person or property, namely (describe the person or property to be seized)

See Attachment B (incorporated by reference herein)

which is (state one or more bases for search and seizure set forth under Rule 41(c) of the Federal Rules of Criminal Procedure)

fruits, instrumentalities and evidence

concerning a violation of Title 18 United States code, Section(s) 2113(a)

The facts to support a finding of probable cause are as follows:

See attached Affidavit of SA Kevin J. Strauss

Continued on the attached sheet and made a part hereof: ☑ Yes ☐ No

Signature of Affiant

Sworn to before me and subscribed in my presence,

MAR 21 2008
Date

at San Diego, California
City State

LEO S. PAPAS
U.S. MAGISTRATE JUDGE
Name of Judge Title of Judge

Signature of Judge

ATTACHMENT A

DESCRIPTION OF PROPERTY TO BE SEARCHED

"Notebook" Laptop Computer
Model M54G "Alienware"
Serial number KA61N4N1N298

currently in the possession of the Federal Bureau of Investigation Evidence Control Center in San Diego, CA.

ATTACHMENT B

ITEMS TO BE SEIZED:

Authorization is sought to search for the evidence of bank robbery in violation of Title 18, United States Code, Section 2113(a). The authorization includes the search of electronic data to include deleted data, remnant data and slack space. The seizure and search of computers and computer media will be conducted in accordance with paragraph 16 of the affidavit submitted in support of this warrant. Evidence to be seized includes but is not limited to:

a. All temporary and permanent files and records of any kind relating to the commission of bank robbery including but not limited to computer logs, database files and communications;

b. All temporary and permanent files and records of any kind, including computer code, computer logs and documents, photographs, email relating to the commission of bank robbery;

c. All temporary and permanent files and records of any kind regarding Bank of America, or other commercial banks, credit unions, and other financial institutions;

d. All records and documents that relate to the obtaining, secreting, transfer, expenditure and/or concealment of money and assets derived from the commission of any previous bank robbery, including receipts for significant purchases, records, bank statements and records, credit card statements and records, business records, money drafts, money orders and cashiers receipts and records of safety deposit boxes and storage lockers; and,

e. All records and documents that identify the dominion and control of the search premises and Internet services at the search premises.

SOUTHERN DISTRICT OF CALIFORNIA

AFFIDAVIT OF KEVIN J. STRAUSS

I, Kevin J. Strauss, being duly sworn, depose and state the following:

1. I make this affidavit in support of an application for a search warrant in furtherance of a bank robbery investigation conducted by Special Agents of the Federal Bureau of Investigation and San Diego Police Department for the following target locations: one Sprint Samsung flip phone, serial number 03215457966/20EBDEAE with photo capabilities seized from Josiah Jorel Jackman; and one Notebook laptop computer, Model M54G "Alienware," serial number KA61N4N1N298 seized from Jackman's residence.

2. Based upon my experience and training, and all the facts and opinions set forth in this Affidavit, I believe items will be found in the cellular telephone and computer to be searched which evidences (1) the existence of the commission of, or conspiracy for the commission of, bank robbery in violation of 18 U.S.C. §2113(a), (2)contraband, fruits of crime or things otherwise criminally possessed, and (3) property designed or intended for use or which is or has been used as a means of committing criminal offenses. See Attachment B for list of items to be seized.

3. The information contained in this affidavit is based on my experience and training, consultation with other special agents of the Federal Bureau of Investigation (FBI), San Diego Police Department (SDPD), and other federal agents

and state law enforcement officers. The evidence and information contained herein was developed from interviews, documents, agency reports, and public records.

I.

EXPERIENCE AND TRAINING

4. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI). I have been employed by the FBI for approximately three years. I am currently assigned to the FBI Violent Crimes Squad, San Diego, California.

5. During my three years with the FBI, I have been involved in numerous investigations related to a wide variety of suspected criminal activity including narcotics trafficking, money laundering, bank robberies, kidnaping, assaults on federal officers, and murder-for-hire. Through my training, education and experience, I have become familiar with the methods of operation used by bank robbers. I am familiar with, and have participated in, all of the normal methods of investigation including, but not limited to, visual surveillance, questioning of witnesses, the use of search and arrest warrants, the use of confidential sources and informants, the use of pen registers, the use of court authorized wire intercepts, and the use of undercover agents.

II.

DETAILS OF THE INVESTIGATION

The following statements are based on my own investigation of the criminal activity described herein, investigation by other federal agents and local law enforcement officers, as well as my experience, training, and

background as a Special Agent with the FBI. Since this affidavit is submitted for a limited purpose, I have not included every fact I know about this investigation. I set forth only the facts necessary to establish foundation for the requested warrants.

6. On Friday, February 29, 2008, at approximately 4:15 p.m., I responded to the report of a robbery at the Bank of America located at 7404 Jackson Drive, San Diego, California.

7. I interviewed the victim teller who advised as follows: On Friday, February 29, 2008, the victim teller was at her teller station when a lone male, later identified as JOSIAH JOREL JACKMAN, vaulted the teller counter top and loudly stated, "This is a robbery." JACKMAN ordered all three tellers working behind the counter at that time to open both their top and bottom cash drawers. JACKMAN grabbed stacks of cash out of the cash drawers one by one while repeatedly ordering the tellers to stand back. Within the money JACKMAN took were three concealed electronic tracking devices. Thereafter, he vaulted back over the counter and departed the bank. The teller described JACKMAN as a 6 foot male wearing a grey, long sleeved hooded sweatshirt, gloves, and a reddish cloth-type material over his face.

8. I learned the following from Officer Reichner, SDPD: On Friday, February 29, 2008, Officer Reichner and his partner responded to the report of a robbery at the Bank of America, 7404 Jackson Drive, San Diego, California. Officer Reichner was updated on JACKMAN's position based on the

signal received from the electronic tracking device JACKMAN took from the bank. At approximately 4:29 p.m. (almost 15 minutes after the robbery), Officer Reichner and his partner found and detained JACKMAN while seated in a red Pontiac Grand Am. The vehicle was parked in a commercial area near 6500 Riverdale Drive, San Diego, California. During an inventory search of the car incident to JACKMAN's arrest, a backpack with U.S. currency totaling $32,486.00 was found on the front passenger side floor area. Included in that money were three concealed electronic tracking devices. Some of the money had spilled out of the backpack onto the car floor area. In the trash dumpster next to where JACKMAN was parked, the grey hooded sweatshirt and reddish cloth JACKMAN wore while robbing the bank were found. A witness from the bank, who had seen JACKMAN remove the red cloth from his face after exiting the bank, positively identified JACKMAN as the bank robber during a curbside lineup. Officer Reichner then transported JACKMAN to the SDPD Headquarters.

9. JACKMAN was searched by SDPD. Target cellular telephone was located on the person of JACKMAN in his pocket. The cellular telephone was seized and transported to the San Diego Division FBI Evidence Control Center where it is being secured.

10. On Friday, February 29, 2008, I interviewed JACKMAN at the SDPD Headquarters. After being advised of his Miranda Rights, JACKMAN voluntarily provided the following statement: On February 28 and 29, 2008, JACKMAN prepared for the bank robbery, i.e., he admitted to cutting a "beanie hat"

into a mask. In addition, JACKMAN stated that he drove his roommate, James Cook, to work so that he would have access to Cook's Pontiac Grand Am. On Friday, February 29, 2008, JACKMAN drove to an area near the Bank of America located at 7404 Jackson Drive, San Diego, California and parked the Pontiac Grand Am. JACKMAN walked to a bench near the bank and watched the bank for several hours before entering. Thereafter, he entered the bank, vaulted the counter, announced that he was robbing the bank, and ordered all three tellers to open their top and bottom cash drawers. The victim tellers complied with JACKMAN's demands and JACKMAN proceeded to grab handfuls of cash from each open drawer. JACKMAN placed the loot from the teller drawers into a backpack he carried into the bank. Thereafter, JACKMAN vaulted back over the counter and fled the bank on foot with the cash. As JACKMAN departed the bank, he took off his cloth mask and ran to the Grand Am. JACKMAN departed the residential area, drove and parked in nearby commercial area. While in the Grand Am, JACKMAN was approached and detained by the police.

11. Also during his interview, JACKMAN was asked if he had ever discussed robbing banks with anyone before the Bank of America robbery. JACKMAN replied that he and his friends would often joke around about robbing banks. They would also go as far as to state how they would go about robbing a bank if they were to do it.

12. JACKMAN used a Pontiac Grand Am owned by his roommate, James Cook, on the day of the robbery.

13. At the end of the interview, JACKMAN gave

consent to the FBI and SDPD to search his premises, specifically his area/room, located at 6532 Reflection Drive, San Diego, California. A "Notebook" laptop computer (target computer) was located in the common area, i.e. living room table, of the apartment. JACKMAN's roommate, James Cook, identified the laptop as being JACKMAN's. Pursuant to the consensual search, JACKMAN's laptop computer was seized.

14. In addition, a Sony Cybershot 7.2 digital camera was discovered in JACKMAN's bedroom in his bedside dresser. A review of the photographs on the digital camera's memory revealed photographs of JACKMAN posing with large amounts of cash. The date stamp on the digital photographs indicate December 2007. A copy of some of the photographs have been attached to this affidavit. (See Exhibit 1 attached hereto.)

15. I assisted in the consent search of JACKMAN's apartment. After a review of the photographs, it appears as if the above referenced photographs (Exhibit 1) were taken inside JACKMAN's apartment located at 6532 Reflection Drive, San Diego, California.

III.

BASIS FOR EVIDENCE SOUGHT IN SEARCH WARRANTS

16. Through my training and experience, and in consultation with other agents and informants, I have learned that:

a. Bank robbers may communicate via cellular telephones and store the names and telephone numbers of other people involved in bank robberies in the memory of the cellular telephones.

b. Bank robbers may utilize cellular telephones with photo capabilities to take photographs and videos of co-conspirators, money, assets purchased with bank robbery proceeds, and targeted banks.

c. Bank robbers may utilize the text or email functions on cellular telephones in the planning and/or commission of the crime.

d. Bank robbers may utilize computers in the preparation, planning, and organization of bank robberies including use of e-mail to communicate with co-conspirators; creation of bank robbery plans; creation of bank robbery notes; storage of photographs and videos of co-conspirators, money, assets purchased with bank robbery proceeds, and targeted banks; internet searches for identification of targeted bank; internet searches for identification of get-a-way routes such as "mapquest"; and storage of financial data related to bank robbery proceeds.

17. JACKMAN admitted that he spent at least two hours on a bench watching the bank prior to robbing it. Based on my training and experience, bank robbers often spend time surveilling or "casing" banks prior to committing a robbery. Based on my training and experience, I believe it is possible that JACKMAN used his cellular telephone to communicate with others, either by telephone call or text message, prior to robbing the bank. In addition, it is possible that JACKMAN used his cellular telephone to take photographs in preparation for the commission of the bank robbery. This information and evidence may be stored on the phone's memory.

18. Furthermore, JACKMAN was detained by SDPD approximately 15 minutes after the commission of the robbery. During this time, JACKMAN had access to his cellular telephone to send/receive telephone calls and text messages as well as use the camera function on his telephone.

IV.

COMPUTER SEARCH PROTOCOL

19. With the approval of the court in signing this warrant, agents executing this search warrant will employ the following procedures regarding computers that may be found on the premises which may contain information subject to seizure pursuant to this warrant:

Forensic Imaging

a. There is probable cause to believe that any computers encountered during this search contain data that, in addition to being evidence of the enumerated crimes as provided at Rule 41(c)(1), Fed.R.Crim.P., are instrumentalities of the offenses in that there is probable cause to believe that they may contain contraband and fruits of crime as provided at Rule 41(c)(2)and/or were used in committing crime as provided at Rule 41(c)(3). Consequently, the computer equipment, including any external storage devices are subject to seizure and will be seized and transported offsite for imaging. A preliminary analysis of the images will be conducted within thirty (30) days to confirm that the computers either contain contraband or were used in committing the subject offenses. If so, the computers will not be returned. If not, any computer without obvious evidence of containing contraband or of being used in the

commission of the enumerated offenses will be returned to its owner. For computers that are retained, the owner may apply in writing to the undersigned for return of specific data not otherwise subject to seizure for which the owner has a specific need. The [seizing agency] will reply in writing. In the event that the owner's request is granted, arrangements will be made for a copy of the requested data to be obtained by the owner. If the request is denied, the owner will be directed to Rule 41(g), Federal Rules of Criminal Procedure.

b. A forensic image is an exact physical copy of the hard drive or other media. It is essential that a forensic image be obtained prior to conducting any search of the data for information subject to seizure pursuant to this warrant. A forensic image captures all of the data on the hard drive or other media without the data being viewed and without changing the data in any way. This is in sharp contrast to what transpires when a computer running the common Windows operating system is started, if only to peruse and copy data - data is irretrievably changed and lost. Here is why: When a Windows computer is started, the operating system proceeds to write hundreds of new files about its status and operating environment. These new files may be written to places on the hard drive that may contain deleted or other remnant data. That data, if overwritten, is lost permanently. In addition, every time a file is accessed, unless the access is done by trained professionals using special equipment, methods and software, the operating system will re-write the metadata for that file. Metadata is

information about a file that the computer uses to manage information. If an agent merely opens a file to look at it, Windows will overwrite the metadata which previously reflected the last time the file was accessed. The lost information may be critical.

c. Special software, methodology and equipment is used to obtain forensic images. Among other things, forensic images normally are "hashed," that is, subjected to a mathematical algorithm to the granularity of 1038 power, an incredibly large number much more accurate than the best DNA testing available today. The resulting number, known as a "hash value" confirms that the forensic image is an exact copy of the original and also serves to protect the integrity of the image in perpetuity. Any change, no matter how small, to the forensic image will affect the hash value so that the image can no longer be verified as a true copy.

Forensic Analysis

d. After obtaining a forensic image, the data will be analyzed. Analysis of the data following the creation of the forensic image is a highly technical process that requires specific expertise, equipment and software. There are literally thousands of different hardware items and software programs that can be commercially purchased, installed and custom-configured on a user's computer system. Computers are easily customized by their users. Even apparently identical computers in an office environment can be significantly different with respect to configuration, including permissions and access rights, passwords, data storage and security. It is not unusual for a computer

forensic examiner to have to obtain specialized hardware or software, and train with it, in order to view and analyze imaged data.

e. Analyzing the contents of a computer, in addition to requiring special technical skills, equipment and software also can be very tedious. It can take days to properly search a single hard drive for specific data. Searching by keywords, for example, often yields many thousands of "hits," each of which must be reviewed in its context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant "hit" does not end the review process. As mentioned above, the computer may have stored information about the data at issue: who created it, when it was created, when was it last accessed, when was it last modified, when was it last printed and when it was deleted. Sometimes it is possible to recover an entire document that never was saved to the hard drive if the document was printed. Operation of the computer by non-forensic technicians effectively destroys this and other trace evidence. Moreover, certain file formats do not lend themselves to keyword searches. Keywords search text. Many common electronic mail, database and spreadsheet applications do not store data as searchable text. The data is saved in a proprietary non-text format. Microsoft Outlook data is an example of a commonly used program which stores data in a non-textual, proprietary manner-ordinary keyword searches will not reach this data. Documents printed by the computer, even if the document never was saved to the hard drive, are recoverable by forensic examiners but not discoverable by

keyword searches because the printed document is stored by the computer as a graphic image and not as text. Similarly, faxes sent to the computer are stored as graphic images and not as text.

f. Analyzing data on-site has become increasingly impossible as the volume of data stored on a typical computer system has become mind-boggling. For example, a single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Computer hard drives are now capable of storing more than 100 gigabytes of data and are commonplace in new desktop computers. And, this data may be stored in a variety of formats or encrypted. The sheer volume of data also has extended the time that it takes to analyze data in a laboratory. Running keyword searches takes longer and results in more hits that must be individually examined for relevance. Even perusing file structures can be laborious if the user is well-organized. Producing only a directory listing of a home computer can result in thousands of pages of printed material most of which likely will be of limited probative value.

g. Based on the foregoing, searching any computer or forensic image for the information subject to seizure pursuant to this warrant may require a range of data analysis techniques and may take weeks or even months. Keywords need to be modified continuously based upon the results obtained; criminals can mislabel and hide files and directories, use codes to avoid using keywords, encrypt files, deliberately

misspell certain words, delete files and take other steps to defeat law enforcement. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques reasonably appear necessary to locate and retrieve digital evidence within the scope of this warrant.

h. All forensic analysis of the imaged data will be directed exclusively to the identification and seizure of information within the scope of this warrant.

V.

CONCLUSION

20. Based on my training and experience, consultation with other special agents and law enforcement officers, and all of the facts and opinions set forth in this affidavit, I have probable cause to believe that violations of 18 U.S.C. §2113(a) - bank robbery, have been committed and evidence of the crimes will be found in the cellular telephone and computer seized from JACKMAN (as described in Attachment A of each search warrant). I believe that evidence of other co-conspirators involved in, and associated with, bank robbery, as well as evidence of the commission of bank robberies will be found on the cellular telephone and computer seized from Jackman.

21. Wherefore, your affiant respectfully requests a warrant be issued authorizing FBI Special Agents and task force officers to examine, analyze, and make record of the contents of the information stored in the seized cellular telephone and computer as described in Attachment A of each search warrant.

Executed on March 20, 2008, at 4:05 p.m.

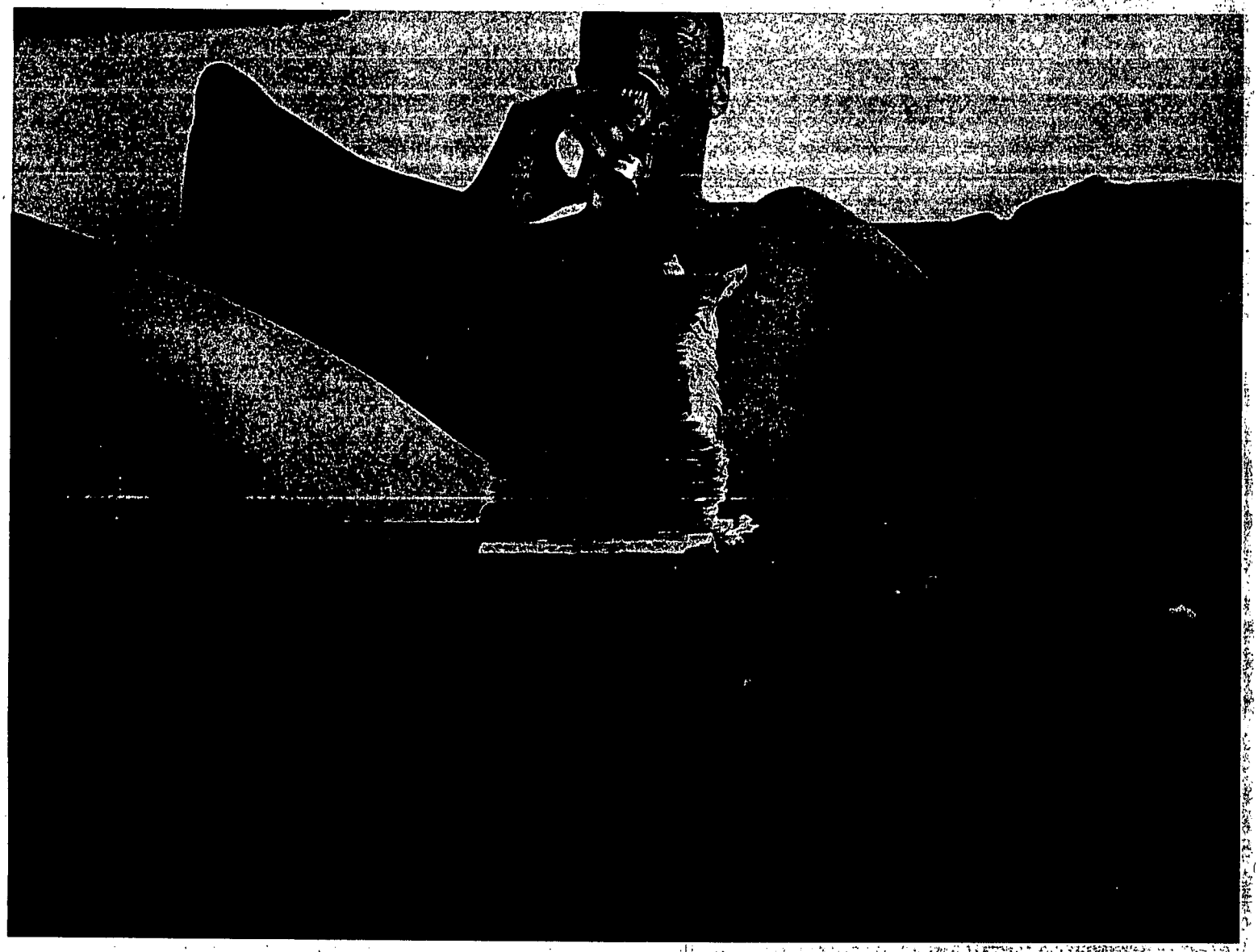
Kevin J. Strauss
Special Agent, FBI

Sworn to and subscribed before me
this 21st day of March, 2008

LEO S. PAPAS
United States Magistrate Judge

MAR 21 2008 4:05
Date/Time

EXHIBIT 1



(Photos Taken Dec 2007)